Practitioner's Docket No. NAI1P458/00.164.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Lee Codel Lawson Tarbotton et al.

Application No.: 09/809,073 Group No.: 2134
Filed: 03/16/2001 Examiner: Simitoski, Michael J.
For: MECHANISMS FOR BANNING COMPUTER PROGRAMS FROM USE

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on 12/12/2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 01/18/2007.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

5. TOTAL FEE DUE

The total fee due is:

Appeal Brief fee	$0.00 (paid previously on December 12, 2005)
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$0.00**

6. FEE PAYMENT

Applicant believes that no fees are due in connection with the filing of this paper because the Appeal Brief fee was paid with a previous submission. However, the commissioner is authorized to charge any fees that may be due to deposit account 50-1351 (Order No. NAI1P458).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351(Order No.NAI1P458).

Date: February 20, 2007

/KEVINZILKA/

Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Tarbotton et al.	Group Art Unit: 2134
Application No. 09/809,073	Examiner: Simitoski, Michael J.
Filed: 03/16/2001	Atty. Docket No.: NAIIP458/00.164.01
For: MECHANISMS FOR BANNING COMPUTER PROGRAMS FROM USE	Date. 02/20/2007

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 12/12/2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 01/18/2007.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, a prior appeal was noted on 12/12/2005 in the present application.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-2, 4-8, 10-16, 18-22, 24-30, 32-36, and 38-46

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-2, 4-8, 10-16, 18-22, 24-30, 32-36, and 38-46
3. Claims allowed: None
4. Claims rejected: 1-2, 4-8, 10-16, 18-22, 24-30, 32-36, and 38-46
5. Claims cancelled: 3, 9, 17, 23, 31, and 37

C. CLAIMS ON APPEAL

The claims on appeal are: 1-2, 4-8, 10-16, 18-22, 24-30, 32-36, and 38-46

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 2-3 et al., a computer program product comprises a computer program operable to control a computer to generate banned program identifying data indicative of at least one computer program to be banned from use. The computer program comprises user controlled program specifying logic which is operable to specify at least one computer program to be banned from use (e.g. see item 14 of Figure 2, etc.), where at least one computer program comprises a non-virus computer program. Further, the computer program comprises banned program identifying data generating logic which is responsive to the user controlled program specifying logic in order to generate banned program identifying data for at least one computer program to be banned from use (e.g. see item 16 of Figure 2, etc.). The banned program identifying data is operable to control anti computer virus logic to identify computer programs banned from use (e.g. see item 40 of Figure 3, etc.). In addition, the anti computer virus logic identifies computer viruses (e.g. see item 32 of Figure 3, etc.) prior to identifying the computer programs banned from use (e.g. see item 40 of Figure 3, etc.). See, for example, page 2, lines 9-19; page 6, lines 19-21; and page 8, lines 11-12 et al.

With respect to a summary of Claim 7, as shown in Figures 2-3 et al., a computer program product comprises a computer program operable to control a computer to ban from use at least one computer program. The at least one computer program comprises a non-virus computer program. The computer program comprises anti computer virus logic, which is responsive to user generated banned program identifying data for at least one computer program to be banned from use (e.g. see item 14 of Figure 2, etc.), in order to identify computer programs banned from use (e.g. see item 40 of Figure 3, etc.). Further, the anti computer virus logic identifies computer viruses (e.g. see item 32 of Figure 3, etc.) prior to identifying the computer programs banned from use (e.g. see item 40 of Figure 3, etc.). See, for example, page 3, lines 20-25, page 6, lines 19-21; and page 8, lines 11-12 et al.

With respect to a summary of Claim 15, as shown in Figures 2-3 et al., a method of generating banned program identifying data indicative of at least one computer program to be banned from use. The method comprises the step of the user specifying at least one computer program to be banned from use (e.g. see item 14 of Figure 3, etc.), where at least one computer program

comprises a non-virus computer program. Further, the method comprises the step of generating banned program identifying data for at least one computer program to be banned from use (e.g. see item 16 of Figure 2, etc.). The banned program identifying data is operable to control anti computer virus logic to identify computer programs banned from use (e.g. see item 40 of Figure 3, etc.). In addition, the anti computer virus logic identifies computer viruses (e.g. see item 32 of Figure 3, etc.) prior to identifying the computer programs banned from use (e.g. see item 40 of Figure 3, etc.). See, for example, page 2, lines 9-19; page 6, lines 19-21; and page 8, lines 11-12 et al.

With respect to a summary of Claim 21, as shown in Figures 2-3 et al., a method for banning from use at least one computer program comprising a non-virus computer program. The method comprises the step of, in response to receiving user generated banned program identifying data for at least one computer program to be banned from use (e.g. see item 14 of Figure 2, etc.), operating anti computer virus logic to identify computer programs banned from use (e.g. see item 40 of Figure 3, etc.) for triggering a banned program action (e.g. see item 44 of Figure 3, etc.). Further, the anti computer virus logic identifies computer viruses (e.g. see item 32 of Figure 3, etc.) prior to identifying the computer programs banned from use (e.g. see item 40 of Figure 3, etc.). See, for example, page 3, lines 20-25; page 4, lines 5-9; page 6, lines 19-21; and page 8, lines 11-12 et al.

With respect to a summary of Claim 29, as shown in Figures 2-3 et al., an apparatus for generating banned program identifying data indicative of at least one computer program to be banned from use comprises a user controlled program specifier operable to specify at least one computer program to be banned from use (e.g. see item 14 of Figure 2, etc.), where at least one computer program comprises a non-virus computer program. Further, the apparatus comprises a banned program identifying data generator, which is responsive to the user controlled program specifier, in order to generate banned program identifying data for at least one computer program to be banned from use (e.g. see item 16 of Figure 2, etc.). The banned program identifying data is operable to control anti computer virus logic to identify computer programs banned from use (e.g. see item 40 of Figure 3, etc.). In addition, the anti computer virus logic identifies computer viruses (e.g. see item 32 of Figure 3, etc.) prior to identifying the computer programs banned

from use (e.g. see item 40 of Figure 3, etc.). See, for example, page 2, lines 9-19; page 6, lines 19-21; and page 8, lines 11-12 et al.

With respect to a summary of Claim 35, as shown in Figures 2-3 et al., an apparatus for banning from use at least one computer program comprises a non-virus computer program. The apparatus comprises an anti computer virus system, which is responsive to user generated banned program identifying data for at least one computer program to be banned from use (e.g. see item 14 of Figure 2, etc.), in order to identify computer programs banned from use (e.g. see item 40 of Figure 3, etc.). Further, the anti computer virus system identifies computer viruses (e.g. see item 32 of Figure 3, etc.) prior to identifying the computer programs banned from use (e.g. see item 40 of Figure 3, etc.). See, for example, page 3, lines 20-25; page 6, lines 19-21; and page 8, lines 11-12 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1, 4, 7, 13, 15, 18, 21, 27, 29, 32, 35, 41, and 45 under 35 U.S.C. 102(b) as being anticipated by Kephart (U.S. Patent No. 5,452,442).

Issue # 2: The Examiner has rejected Claims 1, 4, 7, 13, 15, 18, 21, 27, 29, 32, 35, 41, and 45 under 35 U.S.C. 103(a) as obvious over Kephart (U.S. Patent No. 5,452,442).

Issue # 3: The Examiner has rejected Claims 2, 8, 16, 22, 30, and 36 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Szor ("Bad IDEA"), in further view of Simpson ("Cryptography in Everyday Life").

Issue # 4: The Examiner has rejected Claims 5, 19, and 33 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in further view of Veldman ("Heuristic Anti-Virus Technology").

Issue # 5: The Examiner has rejected Claims 10, 24, and 38 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Szor ("Bad IDEA"), in view of Simpson ("Cryptography in Everyday Life"), and in further view of Davis (U.S. Patent No. 5,844,986).

Issue # 6: The Examiner has rejected Claims 11-12, 25-26, and 39-40 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Symantec ("Norton AntiVirus User's Guide").

Issue # 7: The Examiner has rejected Claims 6, 14, 20, 28, 34, and 42 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of McGee et al. (U.S. Patent No. 6,694,434).

Issue # 8: The Examiner has rejected Claim 43 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Lavasoft ("Ad-aware"), and in further view of Fuller et al. (U.S. Patent No. 6,216,112).

Issue # 9: The Examiner has rejected Claim 44 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Lavasoft ("Ad-aware"), in view of Fuller et al. (U.S. Patent No. 6,216,112), and in further view of Brown et al. (U.S. Patent No. 5,859,968).

Issue # 10: The Examiner has rejected Claim 46 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), and in further view of Golds et al. (U.S. Publication No. 2001/0020245).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1, 4, 7, 13, 15, 18, 21, 27, 29, 32, 35, 41, and 45 under 35 U.S.C. 102(b) as being anticipated by Kephart (U.S. Patent No. 5,452,442).

Group #1: Claims 1, 4, 7, 15, 18, 21, 29, 32, and 35

With respect to the independent claims, the Examiner has relied upon an inherency argument with respect to the Kephart reference to make a prior art showing of appellant's claimed technique "wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use" (see this or similar, but not necessarily identical language in the independent claims).

In response, appellant asserts that "[t]o establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

Specifically, appellant respectfully asserts that Col. 5, lines 57-61 from Kephart merely discloses that "the user supplies either (a) a file containing a list of virus signatures to be evaluated **or** (b) one or more files, each containing one or more portions of invariant viral code from which one or more virus signatures are to be extracted" (emphasis added). Clearly, Kephart's disclosure of using one or more portions of invariant viral code to extract virus signatures, fails to even suggest a technique "wherein the anti computer virus logic identifies computer viruses **prior** to identifying the computer programs banned from use" (emphasis added), as claimed by appellant.

In addition, appellant respectfully asserts that Kephart discloses that "[i]n the evaluation mode the procedure starts with a given list of candidate signatures, one or more for each virus" (emphasis added). Kephart further discloses that "the invention has been described above in the context of methods and apparatus for evaluating and extracting signatures of computer viruses and other undesirable software entities" (Col. 18, lines 17-20 – emphasis added). However, Kephart's disclosure of using a list of candidate signatures in the evaluation mode for both computer viruses and other undesirable software entities *teaches away* from appellant's claimed technique "wherein the anti computer virus logic identifies computer viruses **prior** to identifying the computer programs banned from use" (emphasis added), as claimed, since the same evaluation mode in Kephart is used for both computer viruses and other undesirable software entities, without any indication of order.

Thus, there is absolutely no evidence in the Kephart reference that makes it clear that such missing descriptive matter is necessarily present in the Kephart system. In fact, there is even evidence to the contrary. In view of the arguments made hereinabove, any inherency argument has thus been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

In the Office Action mailed 09/12/2006, the Examiner has argued that "since Kephart's invention identifies both virus and non-virus (programs banned from use), it is an inherent feature of the Kephart invention, if run more than once, to identify a program banned from use after identifying a virus." Further, the Examiner has argued that "even if on each pass through the signature list, the viruses were checked last, on the next running of the checker, the program will have identified the banned programs after the previous identification of viruses."

Appellant respectfully disagrees and asserts that Kephart merely discloses that "the invention has been described…in the context of methods and apparatus for evaluating and extracting signatures of computer viruses and other undesirable software entities" (Col. 18, lines 17-20 – emphasis added). However, there is no indication from the cited excerpt that "on the next running of the

checker, the program will have identified the banned programs after the previous identification of viruses," as stated by the Examiner.

Furthermore, the Examiner has generated a hypothetical situation that is simply not addressed in the Kephart reference. In response, appellant asserts that the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). Thus, it is not inherent in Kephart to "identif[y] computer viruses **prior** to identifying the computer programs banned from use" (emphasis added), as claimed by appellant.

In addition, in the Office Action mailed 9/12/2006, the Examiner has argued that "one of ordinary skill in the art would have been motivated to prioritize the identification of viruses before identifying the computer programs banned from use because it is well known to identify the most severe threats first." First, it appears that, by incorporating an obviousness-type argument, the Examiner is improperly applying the *prima facie* case of obviousness in the context of a rejection under 35 U.S.C. 102(b).

Further, appellant respectfully disagrees with such argument, and asserts that simply nowhere in Kephart is there any disclosure of differing degrees of severity between the identification of viruses and the identification of banned computer programs. To this end, the prior art does not even teach the problem solved by appellant. See *Eibel Process Co. v Minnesota & Ontario Paper Co.*, 261 US 45 (1923). See further arguments addressing 103(a) rejection below in the context of Issue #2.

Again, Kephart's mere disclosure of "evaluating and extracting signatures of computer viruses and other undesirable software entities" (Col. 18, lines 18-20 – emphasis added), in no way suggests or renders obvious "identif[ying] computer viruses **prior** to identifying the computer programs banned from use" (emphasis added), as claimed by appellant. Thus, in view of the arguments made hereinabove, any inherency argument has thus been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

The foregoing anticipation criterion has simply not been met by the above reference.

Group #2: Claims 13, 27, and 41

With respect to Claims 13, 27, and 41, the Examiner has relied on Col. 1, lines 35-49; and Col. 2, lines 5-12 from Kephart to make a prior art showing of appellant's claimed technique "wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use."

> **"A widely-used method for the detection of computer viruses and other undesirable software entities is known as a scanner.** A scanner searches through executable files, boot records, memory, and any other areas that might harbor executable code, for the presence of known undesirable software entities. Typically, a human expert examines a particular undesirable software entity in detail and then uses the acquired information to create a method for detecting it wherever it might occur. In the case of computer viruses, Trojan Horses, and certain other types of undesirable software entities, the detection method that is typically used is to search for the presence of one or more short sequences of bytes, referred to as signatures, which occur in that entity." (Col. 1, lines 35-49)
>
> "However, the accelerating rate at which new viruses, and new variations on previously-known viruses, are appearing creates a heavy burden for human experts. Furthermore, the efficacy of virus scanning is impaired by the time delay between when a virus is first introduced into the world's computer population and when a signature capable of recognizing the virus is distributed to an appreciable fraction of that population." (Col. 2, lines 5-12)

Appellant respectfully asserts that the excerpts from Kephart relied upon by the Examiner merely disclose that "[a] widely-used method for the detection of computer viruses and other undesirable software entities is known as a scanner" (emphasis added). However, the mere

disclosure that a scanner detects computer viruses and other undesirable software entities, as in Kephart, simply fails to even suggest a technique "wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use" (emphasis added), as claimed by appellant.

In addition, appellant respectfully notes that in the Office Action mailed 9/12/2006, the Examiner has even admitted that Kephart inherently teaches that "the second execution will have identified non-viruses after viruses because it identifies both each time" (see page 6 of the Office Action-emphasis added). Clearly, identifying both non-viruses and viruses during each execution of a program, as admitted by the Examiner, does not meet, and even *teaches away* from appellant's claimed technique "wherein said anti computer virus logic is executable as a separate instance **solely** to identify computer programs banned from use" (emphasis added), as claimed.

Again, the foregoing anticipation criterion has simply not been met by the above reference.

Group #3: Claim 45

With respect to Claim 45, the Examiner has relied on Col. 5, lines 57-61 from the Kephart reference, and an inherency argument to make a prior art showing of appellant's claimed technique "wherein the anti computer virus logic of a plurality of end users each includes a different selected set of computer programs banned from use."

Appellant respectfully asserts that the excerpt from Kephart, relied upon by the Examiner to make the foregoing inherency argument, merely discloses that "[i]n a first step, the user supplies either (a) a file containing a list of virus signatures to be evaluated or (b) one or more files, each containing one or more portions of invariant viral code from which one or more virus signatures are to be extracted" (emphasis added). Further, the Examiner has argued that "it is an inherent feature of Kephart that each end user anti computer virus logic includes a different selected set of computer programs (user-selected signatures) banned from use."

Appellant respectfully disagrees, and asserts that Kephart merely discloses that the user supplies "one or more files, each containing one or more portions of invariant viral code" (emphasis added). However, merely disclosing that the user may supply one or more files containing portions of invariant viral code, as in Kephart, fails to even suggest a technique "wherein the anti computer virus logic of a plurality of end users each includes a different selected set of computer programs banned from use" (emphasis added), as claimed by appellant. Clearly, invariant viral code, as in Kephart, fails to suggest "a different selected set of computer programs banned from use" (emphasis added), in the manner as claimed by appellant.

In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Again, the foregoing anticipation criterion has simply not been met by the above reference.

Issue # 2:

The Examiner has rejected Claims 1, 4, 7, 13, 15, 18, 21, 27, 29, 32, 35, 41, and 45 under 35 U.S.C. 103(a) as obvious over Kephart (U.S. Patent No. 5,452,442).

Group #1: Claims 1, 4, 7, 15, 18, 21, 29, 32, and 35

With respect to the independent claims, the Examiner has relied upon an inherency argument with respect to the Kephart reference to make a prior art showing of appellant's claimed technique "wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use" (see this or similar, but not necessarily identical language in the independent claims).

In response, appellant asserts that "[t]o establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may

result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

Specifically, appellant respectfully asserts that Col. 5, lines 57-61 from Kephart merely discloses that "the user supplies either (a) a file containing a list of virus signatures to be evaluated **or** (b) one or more files, each containing one or more portions of invariant viral code from which one or more virus signatures are to be extracted" (emphasis added). Clearly, Kephart's disclosure of using one or more portions of invariant viral code to extract virus signatures, fails to even suggest a technique "wherein the anti computer virus logic identifies computer viruses **prior** to identifying the computer programs banned from use" (emphasis added), as claimed by appellant.

In addition, appellant respectfully asserts that Kephart discloses that "[i]n the evaluation mode the procedure starts with a given list of candidate signatures, one or more for each virus" (emphasis added). Kephart further discloses that "the invention has been described above in the context of methods and apparatus for evaluating and extracting signatures of computer viruses and other undesirable software entities" (Col. 18, lines 17-20 – emphasis added). However, Kephart's disclosure of using a list of candidate signatures in the evaluation mode for both computer viruses and other undesirable software entities *teaches away* from appellant's claimed technique "wherein the anti computer virus logic identifies computer viruses **prior** to identifying the computer programs banned from use" (emphasis added), as claimed, since the same evaluation mode in Kephart is used for both computer viruses and other undesirable software entities, without any indication of order.

Thus, there is absolutely no evidence in the Kephart reference that makes it clear that such missing descriptive matter is necessarily present in the Kephart system. In fact, there is even evidence to the contrary. In view of the arguments made hereinabove, any inherency argument has thus been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

In the Office Action mailed 09/12/2006, the Examiner has argued that "since Kephart's invention identifies both virus and non-virus (programs banned from use), it is an inherent feature of the

Kephart invention, if run more than once, to identify a program banned from use after identifying a virus." Further, the Examiner has argued that "even if on each pass through the signature list, the viruses were checked last, on the next running of the checker, the program will have identified the banned programs after the previous identification of viruses."

Appellant respectfully disagrees and asserts that Kephart merely discloses that "the invention has been described…in the context of methods and apparatus for evaluating and extracting signatures of computer viruses and other undesirable software entities" (Col. 18, lines 17-20 – emphasis added). However, there is no indication from the cited excerpt that "on the next running of the checker, the program will have identified the banned programs after the previous identification of viruses," as alleged by the Examiner.

Furthermore, the Examiner has generated a hypothetical situation that is simply not addressed in the Kephart reference. In response, appellant asserts that the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). Thus, it is not inherent in Kephart to "identif[y] computer viruses **prior** to identifying the computer programs banned from use" (emphasis added), as claimed by appellant.

Again, Kephart's mere disclosure of "evaluating and extracting signatures of computer viruses and other undesirable software entities" (Col. 18, lines 18-20 – emphasis added), in no way suggests or renders obvious "identif[ying] computer viruses **prior** to identifying the computer programs banned from use" (emphasis added), as claimed by appellant. Therefore, in view of the arguments made hereinabove, any inherency argument has thus been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

In addition, in the Office Action mailed 9/12/2006, the Examiner has argued that "one of ordinary skill in the art would have been motivated to prioritize the identification of viruses before identifying the computer programs banned from use because it is well known to identify the most severe threats first." Appellant respectfully disagrees with such argument, and asserts

that simply nowhere in Kephart is there any disclosure of differing degrees of severity between the identification of viruses and the identification of banned computer programs. To this end, the prior art does not even teach the problem solved by appellant. See *Eibel Process Co. v Minnesota & Ontario Paper Co.*, 261 US 45 (1923).

Further, in order to establish a prima facie case of obviousness where the advance in the art lies in the discovery of the problem or source of the problem, as here, the Examiner must provide evidence that a person of ordinary skill in the art at the time of the present invention would have expected a problem to exist. As noted by the court in *In Re Nomiya*, 509 F.2d 566, 572, 184 USPQ 607, 612 (CCPA 1975).

> [Where] there is no evidence of record that a person of ordinary skill in the art at the time of [an appellant's] invention would have expected [a problem],..., it is not proper to conclude that [an invention], which solves this problem...would have been obvious to that hypothetical person of ordinary skill in the art. The significance of evidence that a problem was known in the prior art is, of course, that knowledge of a problem provides a reason or motivation for workers in the art to apply their skill to its solution.

Absent such evidence in the record and a proper rejection under 35 U.S.C. 103(a), the rejection based on the Kephart reference cannot stand.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #2: Claims 13, 27, and 41

With respect to Claims 13, 27, and 41, the Examiner has relied on Col. 1, lines 35-49; and Col. 2, lines 5-12 from Kephart to make a prior art showing of appellant's claimed technique "wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use."

> "**A widely-used method for the detection of computer viruses and other undesirable software entities is known as a scanner.** A scanner searches through executable files, boot records, memory, and any other areas that might harbor executable code, for the presence of known undesirable software entities. Typically, a human expert examines a particular undesirable software entity in detail and then uses the acquired information to create a method for detecting it wherever it might occur. In the case of computer viruses, Trojan Horses, and certain other types of undesirable software entities, the detection method that is typically used is to search for the presence of one or more short sequences of bytes, referred to as signatures, which occur in that entity." (Col. 1, lines 35-49)
>
> "However, the accelerating rate at which new viruses, and new variations on previously-known viruses, are appearing creates a heavy burden for human experts. Furthermore, the efficacy of virus scanning is impaired by the time delay between when a virus is first introduced into the world's computer population and when a signature capable of recognizing the virus is distributed to an appreciable fraction of that population." (Col. 2, lines 5-12)

Appellant respectfully asserts that the excerpts from Kephart relied upon by the Examiner merely disclose that "[a] widely-used method for the detection of computer viruses and other undesirable software entities is known as a scanner" (emphasis added). However, the mere disclosure that a scanner detects computer viruses and other undesirable software entities, as in Kephart, simply fails to even suggest a technique "wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use" (emphasis added), as claimed by appellant.

In addition, appellant respectfully notes that in the Office Action mailed 9/12/2006, the Examiner has even admitted that Kephart inherently teaches that "the second execution will have identified non-viruses after viruses because it identifies both each time" (see page 6 of the Office Action-emphasis added). Clearly, identifying both non-viruses and viruses during each

execution of a program, as noted by the Examiner, does not meet, and even *teaches away* from appellant's claimed technique "wherein said anti computer virus logic is executable as a separate instance **solely** to identify computer programs banned from use" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #3: Claim 45

With respect to Claim 45, the Examiner has relied on Col. 5, lines 57-61 from the Kephart reference, and an inherency argument to make a prior art showing of appellant's claimed technique "wherein the anti computer virus logic of a plurality of end users each includes a different selected set of computer programs banned from use."

Appellant respectfully asserts that the excerpt from Kephart, relied upon by the Examiner to make the foregoing inherency argument, merely discloses that "[i]n a first step, the user supplies either (a) a file containing a list of virus signatures to be evaluated or (b) one or more files, each containing one or more portions of invariant viral code from which one or more virus signatures are to be extracted" (emphasis added). Further, the Examiner has argued that "it is an inherent feature of Kephart that each end user anti computer virus logic includes a different selected set of computer programs (user-selected signatures) banned from use."

Appellant respectfully disagrees, and asserts that Kephart merely discloses that the user supplies "one or more files, each containing one or more portions of invariant viral code" (emphasis added). However, merely disclosing that the user may supply one or more files containing portions of invariant viral code, as in Kephart, fails to even suggest a technique "wherein the anti computer virus logic of a plurality of end users each includes a different selected set of computer programs banned from use" (emphasis added), as claimed by appellant. Clearly, invariant viral code, as in Kephart, fails to suggest "a different selected set of computer programs banned from use" (emphasis added), in the manner as claimed by appellant.

In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 3:

The Examiner has rejected Claims 2, 8, 16, 22, 30, and 36 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Szor ("Bad IDEA"), in further view of Simpson ("Cryptography in Everyday Life").

Group # 1: Claims 2, 8, 16, 22, 30, and 36

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1, and Issue #2, Group #1.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 4:

The Examiner has rejected Claims 5, 19, and 33 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in further view of Veldman ("Heuristic Anti-Virus Technology").

Group # 1: Claims 5, 19, and 33

With respect to Claims 5, 19, and 33, the Examiner has relied on Section 1, and Section 2.1 from the Veldman reference to make a prior art showing of appellant's claimed technique "wherein said banned program identifying data includes heuristic data identifying at least one behavioral

characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified."

Appellant respectfully asserts that the excerpts from Veldman relied upon by the Examiner merely disclose that "[t]he word 'heuristic' means (according to a Dutch dictionary) 'the self finding' and 'the knowledge to determine something in a methodic way'" (Section 2.1). Further, Veldman discloses that "[a] heuristic scanner is a type of automatic debugger or disassembler" where "[t]he instructions are disassembled and their purposes are determined" (Section 2.1). In addition, Veldman discloses that "normal programs typically start searching the command line for options, clearing the screen, etc." where viruses "start with a search for other executable files, by writing to the disk, or by decrypting themselves" (Section 2.1).

However, the mere disclosure of using a heuristic scanner to determine if the instructions are acting in a manner consistent with a virus, such as checking for other executable files, writing to disk, or decrypting themselves, as in Veldman, simply fails to even suggest a technique "wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified" (emphasis added), as claimed by appellant. Clearly, suggesting the use of heuristics to detect instructions indicative of a virus, as in Veldman, simply fails to suggest that the "banned program identifying data **includes** heuristic data identifying at least one behavioral characteristic" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 5:

The Examiner has rejected Claims 10, 24, and 38 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Szor ("Bad IDEA"), in view of Simpson ("Cryptography in Everyday Life"), and in further view of Davis (U.S. Patent No. 5,844,986).

Group #1: Claims 10, 24, and 38

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that "[o]ne of ordinary skill in the art would have been motivated to perform such a modification to prevent a virus from corrupting the identifying data, as taught by Davis (col. 1, lines 32-45 & 63-67)." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of Davis, with the Kephart, Szor, and Simpson references, especially in view of the vast evidence to the contrary.

For example, Kephart relates to "[a] method... to extract and/or evaluate a signature of a computer virus or other undesirable software entity" (Abstract), Szor relates to the analysis of "IDEA.6155 [which is] a polymorphic virus with three layers of encryption" (Page 18, Paragraph 3), and Simpson relates to receiving a message encrypted with a private key which may be decrypted with a public key (Section 1), while Davis relates to "[a] cryptographic coprocessor containing the BIOS memory device [which] performs authentication and validation on the BIOS upgrade based on a public/private key protocol" (Abstract). To simply glean features from a cryptographic coprocessor containing the BIOS memory device, such as that of Davis, and combine the same with the *non-analogous art* of a method of evaluating signatures of computer viruses, such as that of Kephart, a polymorphic virus, such as that of Szor, and private and public key encryption, such as of Simpson, would simply be improper.

In particular, cryptographic coprocessors containing BIOS memory impose an authentication and validation procedure before the contents of the BIOS flash memory are modified (Davis - Col. 1, lines 65-67), while virus scanners evaluate signatures of computer viruses, polymorphic viruses use encryption, and public key cryptography uses private and public keys to encrypt and decrypt messages. "In order to rely on a reference as a basis for rejection of an appellant's invention, the reference must either be in the field of appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61

(Fed. Cir. 1992). In view of the vastly different types of problems a cryptographic coprocessor containing BIOS memory addresses as opposed to a virus scanner, polymorphic virus, and public key cryptography, the Examiner's proposed combination is inappropriate.

Further, with respect to the third element of the prima facie case of obviousness, the Examiner has relied on Col. 1, lines 32-45, and lines 63-67; and Col. 2, lines 1-7 from the Davis reference to make a prior art showing of appellant's claimed technique "wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted."

> 'In this respect, **BIOS implemented in EPROM is resistant to virus attack and other electronic sabotages.** However, EPROM devices do not support "field upgrades" because these devices are not in-circuit programmable, which is a necessary characteristic for field upgrades. Field upgrading allows customers to upgrade the BIOS in the field to avoid costly delay and parts exchanges. Because of the importance for field upgrading, virtually all BIOS firmware is now implemented using flash memories. However, being field modifiable, **BIOS flash memories are vulnerable to virus attacks** which could cause devastating results in sensitive applications such as financial transactions.' (Col. 1, lines 32-45 - emphasis added)
>
> "The primary focus of the present invention, therefore, is to **prevent corrupting the BIOS by a computer virus.** This is **achieved by imposing an authentication and validation procedure before the contents of the BIOS flash memory are modified.**" (Col. 1, lines 63-67 - emphasis added)
>
> "The approach which is pursued in this invention builds on the concept of BIOS authentication by **incorporating the BIOS flash memories into existing hardware with authenticating capability such as the cryptographic coprocessor.** Since the cryptographic coprocessor both stores the BIOS and enforces authentication of BIOS updates, an attacker has no means by which to corrupt the BIOS contents." (Col. 2, lines 1-7 - emphasis added)

Appellant respectfully asserts that the excerpts from Davis relied upon by the Examiner merely disclose that "BIOS implemented in EPROM is resistant to virus attack and other electronic sabotages" and "BIOS flash memories are vulnerable to virus attacks" (emphasis added). Further, Davis discloses that in order to "prevent corrupting the BIOS by a computer virus...an authentication and validation procedure [is imposed] before the contents of the BIOS flash memory are modified" by "incorporating the BIOS flash memories into existing hardware with authenticating capability such as the cryptographic coprocessor" (emphasis added).

However, the mere disclosure that flash memory BIOS, which is vulnerable to virus attacks, is incorporated into existing hardware with authentication capability in order to authenticate and validate before the contents of BIOS flash memory are modified, as in Davis, simply fails to suggest technique "wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted" (emphasis added), as claimed by appellant. Clearly, hardware providing authentication and validation before a BIOS flash memory is modified, as in Davis, simply fails to even suggest that "decrypted banned program identifying data is stored within a secured memory region once decrypted" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 6:

The Examiner has rejected Claims 11-12, 25-26, and 39-40 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Symantec ("Norton AntiVirus User's Guide").

Group #1: Claims 11, 25, and 39

With respect to Claims 11, 25, and 39, the Examiner has relied on Pages 39-40 from the Symantec reference to make a prior art showing of appellant's claimed technique "wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of: (i) issuing an alert message indicating identification of a banned computer program; (ii) denying access to said banned computer program; (iii) encrypting said banned computer program; and (iv) deleting said banned computer program."

Appellant respectfully asserts that the excerpt from Symantec relied upon by the Examiner merely discloses that "[w]hen Norton AntiVirus finds a virus has infected a file on your computer, it produces a warning" (Page 40 – emphasis added). However, the mere disclosure of producing a warning when a virus has infected a file, as in Symantec, simply fails to even suggest a technique "wherein when a banned computer program is identified, at least one banned program action is triggered" (emphasis added), in the manner as claimed by appellant. Clearly, finding a virus that has infected a file, as in Symantec, *teaches away* from appellant's "banned computer program" which "compris[es] a non-virus computer program" (see Claim 1 for context – emphasis added), in the context as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #2: Claims 12, 26, and 40

With respect to Claims 12, 26, and 40, the Examiner has relied on Pages 11, and 18 from the Symantec reference to make a prior art showing of appellant's claimed technique "wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of: (i) issuing an alert message indicating an absence of said user generated banned program identifying data; (ii) restoring said user generated banned program identifying data from a remote source; (iii) disabling a computer upon which said anti computer virus logic is executing."

Appellant respectfully asserts that the excerpts from Symantec relied on by the Examiner merely disclose that "Norton AntiVirus relies on up-to-date information to detect and eliminate viruses" and "[o]ne of the most common reasons you may have a virus problem is that you have not updated your virus protection since you purchased the product" (Page 11). Further, Symantec discloses to "[c]lick the LiveUpdate button to update Norton AntiVirus programs and virus protection" (Page 18). In addition, Symantec discloses that "LiveUpdate connects to Symantec to see if updates are available for Norton AntiVirus and also checks for updates to your virus protection" (Page 18 – emphasis added).

However, the mere disclosure that LiveUpdate connects to Symantec to see if updates are available for Norton AntiVirus and also checks for updates to your virus protection, as in Symantec, simply fails to suggest a technique "wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data" (emphasis added), in the manner as claimed by appellant. Clearly, updating virus protection via LiveUpdate, as in Symantec, does not meet "an **absence** of said **user generated** banned program identifying data" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 7:

The Examiner has rejected Claims 6, 14, 20, 28, 34, and 42 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of McGee et al. (U.S. Patent No. 6,694,434).

Group #1: Claims 6, 14, 20, 28, 34, and 42

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that "it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kephart so that the banned program identifying data identifying permitted compute[r] programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use" and that "[o]ne of ordinary skill in the art would have been motivated to perform such a modification to protect a computer against inadvertently downloaded unauthorized programs, as taught by McGee (col. 2, lines 35-41 & col. 3, line 64 – col. 4, line 4)." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of McGee, with the Kephart reference, especially in view of the vast evidence to the contrary.

For example, Kephart relates to "[a] method... to extract and/or evaluate a signature of a computer virus or other undesirable software entity" (Abstract), while McGee relates to a "system and method for controlling program execution for a first-party" (Col. 1, lines 64-65). To simply glean features from a method for controlling program execution, such as that of McGee, and combine the same with the *non-analogous art* of a method of evaluating signatures of computer viruses, would simply be improper.

In particular, in a method for controlling program execution, the "first-party system grants program executability on a per-program basis based on the comparison of the pre-stored hash values and hash value generated by the party having the program designated for execution" (McGee, Col. 2, lines 26-30 -- emphasis added), while virus scanners extract and evaluate signatures of computer viruses, as in Kephart. "In order to rely on a reference as a basis for rejection of an appellant's invention, the reference must either be in the field of appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F 2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly different types of problems a method for controlling program execution addresses as opposed to a virus scanner, the Examiner's proposed combination is inappropriate.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 8:

The Examiner has rejected Claim 43 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Lavasoft ("Ad-aware"), and in further view of Fuller et al. (U.S. Patent No. 6,216,112).

Group # 1: Claim 43

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that "it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Kephart to use the anti-virus software to remove data streaming programs" and that "[o]ne of ordinary skill in the art would have been motivated to perform such a modification because adware streams data, as taught by Fuller (abstract)." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Fuller, with the Kephart reference, especially in view of the vast evidence to the contrary.

For example, Kephart relates to "[a] method... to extract and/or evaluate a signature of a computer virus or other undesirable software entity" (Abstract), while Fuller relates to "[a] method and system for offering and distributing software wherein advertisements are incorporated into the software product" (Abstract) where "[a] technical advantage achieved with the invention is the ability to couple advertisement software with a separate software program" (Col. 4, lines 56-58). To simply glean features from a method for distributing software with advertisements incorporated into the software product, such as that of Fuller, and combine the same with the *non-analogous art* of a method of evaluating signatures of computer viruses, such as that of Kephart, would simply be improper.

In particular, distributing software with advertisements incorporated into the software product allows for software authors to be compensated for every copy of the software being used (Fuller, Col. 4, lines 56-61), while virus scanners evaluate signatures of computer viruses. "In order to rely on a reference as a basis for rejection of an appellant's invention, the reference must either be in the field of appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly different types of problems a method for distributing software with advertisements incorporated into the software product addresses as opposed to a virus scanner, the Examiner's proposed combination is inappropriate.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 9:

The Examiner has rejected Claim 44 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), in view of Lavasoft ("Ad-aware"), in view of Fuller et al. (U.S. Patent No. 6,216,112), and in further view of Brown et al. (U.S. Patent No. 5,859,968).

Group #1: Claim 44

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that "it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kephart such that the non-virus computer programs further include games" where "[o]ne of ordinary skill in the art would have been motivated to perform such a modification to enable employers to prevent the addition of the games to employee computers, as taught by Brown (col. 4, lines 10-12)" To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Brown, with the Kephart reference, especially in view of the vast evidence to the contrary.

For example, Kephart relates to "[a] method... to extract and/or evaluate a signature of a computer virus or other undesirable software entity" (Abstract), while Brown relates to "[a] data security device for a computer system [that] controls the addition and removal of data using an external data drive" where "[t]he access controller selectively makes or breaks an electrical connection between the power supply and the external data drive to prevent the addition or removal of data from the computer system using the external data drive" (Abstract). To simply glean features from an access controller, such as that of Brown, and combine the same with the *non-analogous art* of a method of evaluating signatures of computer viruses, such as that of Kephart, would simply be improper.

In particular, an access controller makes or breaks an electrical connection between the power supply and the external data drive to prevent the addition or removal of data from the external data drive, while virus scanners evaluate signatures of computer viruses. "In order to rely on a reference as a basis for rejection of an appellant's invention, the reference must either be in the field of appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly different types of problems an access controller addresses as opposed to a virus scanner, the Examiner's proposed combination is inappropriate.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 10:

The Examiner has rejected Claim 46 under 35 U.S.C. 103(a) as being unpatentable over Kephart (U.S. Patent No. 5,452,442), and in further view of Golds et al. (U.S. Publication No. 2001/0020245).

Group #1: Claim 46

With respect to Claim 46, the Examiner has relied on Paragraphs 0003, 0008, and 0031 in Golds to make a prior art showing of appellant's claimed technique "wherein an anti-virus scan is performed when a file access request is received, and if said anti-virus scan is not passed, an anti-virus action is triggered and a fail response is returned to an operating system, and if said anti-virus scan is passed, a scan for the computer programs banned from use is performed."

Appellant respectfully asserts that the excerpts from Golds relied upon by the Examiner merely disclose that "[s]oftware modules such as file system filter drivers may be stacked or otherwise arranged linearly (e.g., chained), and perform their operations in the order in which they are

stacked" (emphasis added). Additionally, Golds discloses that "the drivers can intercept IRPs [(I/O request packets)], and modify, return and/or cancel them" (emphasis added).

However, the mere disclosure that file system filter drivers may be arranged linearly and that the drivers can intercept, modify, return, and/or cancel IRPs, as in Golds, fails to even suggest a technique "wherein an anti-virus scan is performed when a file access request is received, and if said anti-virus scan is not passed, an anti-virus action is triggered and a fail response is returned to an operating system, and if said anti-virus scan is passed, a scan for the computer programs banned from use is performed" (emphasis added), as claimed by appellant. Clearly, the excerpts from Golds relied upon by the Examiner fail to even suggest that "if said anti-virus scan is passed, a scan for the computer programs banned from use is performed" (emphasis added), as claimed by appellant.

In addition, the Examiner has argued that "it is inherent in Kephart that all signatures will be scanned and therefore, if one signature does not match a file, the next will be checked...[and that] since Kephart scans a file with respect to virus and non-virus files, it is inherent that when a virus signature does not match the file being scanned, the file will be scanner or the remaining signatures, at least one corresponding to a non-virus file." Appellant respectfully disagrees with the Examiner's inherency arguments and asserts that Kephart merely discloses that "the invention has been described...in the context of methods and apparatus for evaluating and extracting signatures of computer viruses and other undesirable software entities" (Col. 18, lines 17-20 – emphasis added). However, there is no indication from the cited excerpt that "if one signature does not match a file, the next will be checked," and "when a virus signature does not match the file being scanned, the file will be scanned for the remaining signatures, at least one corresponding to a non-virus file," as stated by the Examiner. Clearly, evaluating signatures of computer viruses and other undesirable software entities, as in Kephart, simply fails to specifically suggest that "if said anti-virus scan is passed, a scan for the computer programs banned from use is performed" (emphasis added), in the manner as claimed by appellant.

Appellant asserts that the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993); *In re Oelrich*, 666 F.2d 578, 581-

82, 212 USPQ 323, 326 (CCPA 1981). Thus, it is not inherent in Kephart that "if said anti-virus scan is passed, a scan for the computer programs banned from use is performed" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product comprising a computer program operable to control a computer to generate banned program identifying data indicative of at least one computer program to be banned from use, said computer program comprising:
(i) user controlled program specifying logic operable to specify said at least one computer program to be banned from use, said at least one computer program comprising a non-virus computer program; and
(ii) banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use;
wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use.

2. (Original) A computer program product as claimed in claim 1, wherein said banned program identifying data is encrypted with a private key.

3. (Cancelled)

4. (Previously Presented) A computer program product as claimed in claim 1, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were one of the computer viruses.

5. (Previously Presented) A computer program product as claimed in claim 4, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least

one computer program banned from use that share said behavioral characteristics may also be identified

6. (Original) A computer program product as claimed in claim 1, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

7. (Previously Presented) A computer program product comprising a computer program operable to control a computer to ban from use at least one computer program, said at least one computer program comprising a non-virus computer program, said computer program comprising:

(i) anti computer virus logic responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use.

8. (Original) A computer program product as claimed in claim 7, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

9. (Cancelled)

10. (Original) A computer program product as claimed in claim 8, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

11. (Previously Presented) A computer program product as claimed in claim 7, wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

12. (Original) A computer program product as claimed in claim 7, wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

13. (Original) A computer program product as claimed in claim 7, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

14. (Original) A computer program product as claimed in claim 7, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

15. (Previously Presented) A method of generating banned program identifying data indicative of at least one computer program to be banned from use, said method comprising the steps of:

(i) user specifying at least one computer program to be banned from use, said at least one computer program comprising a non-virus computer program; and

(ii) generating banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use

16. (Original) A method as claimed in claim 15, wherein said banned program identifying data is encrypted with a private key.

17. (Cancelled)

18. (Previously Presented) A method as claimed in claim 15, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were one of the computer viruses.

19. (Previously Presented) A method as claimed in claim 18, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified.

20. (Original) A method as claimed in claim 15, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

21. (Previously Presented) A method for banning from use at least one computer program, said at least one computer program comprising a non-virus computer program, said method comprising the step of:

(i) in response to receiving user generated banned program identifying data for said at least one computer program to be banned from use, operating anti computer virus logic to identify computer programs banned from use for triggering a banned program action;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use.

22. (Original) A method as claimed in claim 21, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

23. (Cancelled)

24. (Original) A method as claimed in claim 22, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

25. (Previously Presented) A method as claimed in claim 21, wherein when a banned computer program is identified, said at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

26. (Original) A method as claimed in claim 21, wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

27. (Original) A method as claimed in claim 21, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

28. (Original) A method as claimed in claim 21, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

29. (Previously Presented) Apparatus for generating banned program identifying data indicative of at least one computer program to be banned from use, said apparatus comprising:

(i) a user controlled program specifier operable to specify at least one computer program to be banned from use, said at least one computer program comprising a non-virus computer program; and

(ii) banned program identifying data generator responsive to said user controlled program specifier to generate banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use.

30. (Original) Apparatus as claimed in claim 29, wherein said banned program identifying data is encrypted with a private key.

31. (Cancelled)

32. (Previously Presented) Apparatus as claimed in claim 29, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were one of the computer viruses.

33. (Previously Presented) Apparatus as claimed in claim 32, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified.

34. (Original) Apparatus as claimed in claim 29, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

35. (Previously Presented) Apparatus for banning from use at least one computer program, said at least one computer program comprising a non-virus computer program, said apparatus comprising:

(i) an anti computer virus system responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use;

wherein the anti computer virus system identifies computer viruses prior to identifying the computer programs banned from use.

36. (Original) Apparatus as claimed in claim 35, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

37. (Cancelled)

38. (Original) Apparatus as claimed in claim 36, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

39. (Previously Presented) Apparatus as claimed in claim 35, wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

40. (Original) Apparatus as claimed in claim 35, wherein said anti computer virus system responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

41. (Original) Apparatus as claimed in claim 35, wherein said anti computer virus system is executable as a separate instance solely to identify computer programs banned from use.

42. (Original) Apparatus as claimed in claim 35, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

43. (Previously Presented) A computer program product as claimed in claim 1, wherein the at least one non-virus computer program includes at least one of a game and a data streaming program.

44. (Previously Presented) A computer program product as claimed in claim 1, wherein the at least one non-virus computer program includes games and data streaming programs.

45. (Previously Presented) A computer program product as claimed in claim 1, wherein the anti computer virus logic of a plurality of end users each includes a different selected set of computer programs banned from use.

46. (Previously Presented) A computer program product as claimed in claim 1, wherein an anti-virus scan is performed when a file access request is received, and if said anti-virus scan is not passed, an anti-virus action is triggered and a fail response is returned to an operating system, and if said anti-virus scan is passed, a scan for the computer programs banned from use is performed.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P458).

Respectfully submitted,

By: /KEVINZILKA/ Date: February 20, 2007

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660